

115TH CONGRESS
1ST SESSION

H. R. 3816

To require notification following a breach of security of a system containing personal information, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

SEPTEMBER 21, 2017

Mr. RUSH introduced the following bill; which was referred to the Committee on Energy and Commerce

A BILL

To require notification following a breach of security of a system containing personal information, and for other purposes.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. NOTIFICATION OF INFORMATION SECURITY**
4 **BREACH.**

5 (a) NATIONWIDE NOTIFICATION.—Any person en-
6 gaged in interstate commerce that owns or possesses data
7 in electronic form containing personal information shall,
8 following the discovery of a breach of security of the sys-
9 tem maintained by such person that contains such data—

- 1 (1) notify each individual who is a citizen or
2 resident of the United States whose personal infor-
3 mation was acquired or accessed as a result of such
4 a breach of security;
5 (2) notify the Commission; and
6 (3) notify the Bureau.

7 (b) SPECIAL NOTIFICATION REQUIREMENTS.—

8 (1) THIRD-PARTY AGENTS.—In the event of a
9 breach of security by any third-party entity that has
10 been contracted to maintain or process data in elec-
11 tronic form containing personal information on be-
12 half of any other person who owns or possesses such
13 data, such third-party entity shall be required to no-
14 tify such person of the breach of security. Upon re-
15 ceiving such notification from such third party, such
16 person shall provide the notification required under
17 subsection (a).

18 (2) SERVICE PROVIDERS.—If a service provider
19 becomes aware of a breach of security of data in
20 electronic form containing personal information that
21 is owned or possessed by another person that con-
22 nects to or uses a system or network provided by the
23 service provider for the purpose of transmitting,
24 routing, or providing intermediate or transient stor-
25 age of such data, such service provider shall be re-

1 quired to notify of such a breach of security only the
2 person who initiated such connection, transmission,
3 routing, or storage if such person can be reasonably
4 identified. Upon receiving such notification from a
5 service provider, such person shall provide the notifi-
6 cation required under subsection (a).

7 (3) COORDINATION OF NOTIFICATION WITH
8 CONSUMER REPORTING AGENCIES.—If a person is
9 required to provide notification to more than 1,000
10 individuals under subsection (a)(1), the person shall
11 also notify the major consumer reporting agencies of
12 the timing and distribution of the notices. Such no-
13 tice shall be given to the consumer reporting agen-
14 cies without unreasonable delay and, if it will not
15 delay notice to the affected individuals, prior to the
16 distribution of notices to the affected individuals.

17 (c) TIMELINESS OF NOTIFICATION.—

18 (1) IN GENERAL.—Unless subject to a delay au-
19 thorized under paragraph (2), a notification required
20 under subsection (a) shall be made not later than 30
21 days following the discovery of a breach of security,
22 unless the person providing notice can show that
23 providing notice within such a timeframe is not fea-
24 sible due to extraordinary circumstances necessary
25 to prevent further breach or unauthorized disclo-

1 sures, and reasonably restore the integrity of the
2 data system, in which case such notification shall be
3 made as promptly as possible.

4 (2) DELAY OF NOTIFICATION AUTHORIZED FOR
5 LAW ENFORCEMENT OR NATIONAL SECURITY PUR-
6 POSES.—

7 (A) LAW ENFORCEMENT.—If a Federal,
8 State, or local law enforcement agency deter-
9 mines that the notification required under this
10 section would impede a civil or criminal inves-
11 tigation, such notification shall be delayed upon
12 the written request of the law enforcement
13 agency for 30 days or such lesser period of time
14 which the law enforcement agency determines is
15 reasonably necessary and requests in writing. A
16 law enforcement agency may, by a subsequent
17 written request, revoke such delay or extend the
18 period of time set forth in the original request
19 made under this paragraph if further delay is
20 necessary.

21 (B) NATIONAL SECURITY.—If a Federal
22 national security agency or homeland security
23 agency determines that the notification required
24 under this section would threaten national or
25 homeland security, such notification may be de-

1 laid for a period of time which the national se-
2 curity agency or homeland security agency de-
3 termines is reasonably necessary and requests
4 in writing. A Federal national security agency
5 or homeland security agency may revoke such
6 delay or extend the period of time set forth in
7 the original request made under this paragraph
8 by a subsequent written request if further delay
9 is necessary.

10 (d) METHOD AND CONTENT OF NOTIFICATION.—

11 (1) DIRECT NOTIFICATION.—

12 (A) METHOD OF NOTIFICATION.—A person
13 required to provide notification to individuals
14 under subsection (a)(1) shall be in compliance
15 with such requirement if the person provides
16 conspicuous and clearly identified notification
17 by one of the following methods (provided the
18 selected method can reasonably be expected to
19 reach the intended individual):

20 (i) Written notification.

21 (ii) Notification by email or other
22 electronic means, if—

23 (I) the person's primary method
24 of communication with the individual

1 is by email or such other electronic
2 means; or

3 (II) the individual has consented
4 to receive such notification and the
5 notification is provided in a manner
6 that is consistent with the provisions
7 permitting electronic transmission of
8 notices under section 101 of the Elec-
9 tronic Signatures in Global and Na-
10 tional Commerce Act (15 U.S.C.
11 7001).

12 (B) CONTENT OF NOTIFICATION.—Regard-
13 less of the method by which notification is pro-
14 vided to an individual under subparagraph (A),
15 such notification shall include—

16 (i) a description of the personal infor-
17 mation that was acquired or accessed by
18 an unauthorized person;

19 (ii) a telephone number that the indi-
20 vidual may use, at no cost to such indi-
21 vidual, to contact the person to inquire
22 about the breach of security or the infor-
23 mation the person maintained about that
24 individual;

(iii) notice that the individual is entitled to receive, at no cost to such individual, consumer credit reports on a quarterly basis for a period of 5 years, credit monitoring or other service that enables consumers to detect the misuse of their personal information for a period of 10 years, and instructions to the individual on requesting such reports or service from the person, except when the only information which has been the subject of the security breach is the individual's first name or initial and last name, or address, or phone number, in combination with a credit or debit card number, and any required security code;

(iv) the toll-free contact telephone numbers and addresses for the major consumer reporting agencies;

(v) a toll-free telephone number and Internet website address for the Commission whereby the individual may obtain information regarding identity theft; and

(vi) a toll-free telephone number and Internet website address for the Bureau

1 whereby the individual may obtain infor-
2 mation regarding identity theft and credit
3 reports.

4 (2) SUBSTITUTE NOTIFICATION.—

5 (A) CIRCUMSTANCES GIVING RISE TO SUB-
6 STITUTE NOTIFICATION.—A person required to
7 provide notification to individuals under sub-
8 section (a)(1) may provide substitute notifica-
9 tion in lieu of the direct notification required by
10 paragraph (1) if the person owns or possesses
11 data in electronic form containing personal in-
12 formation of fewer than 1,000 individuals and
13 such direct notification is not feasible due to—

14 (i) excessive cost to the person re-
15 quired to provide such notification relative
16 to the resources of such person, as deter-
17 mined in accordance with the regulations
18 issued by the Commission under paragraph
19 (3)(A); or

20 (ii) lack of sufficient contact informa-
21 tion for the individual required to be noti-
22 fied.

23 (B) FORM OF SUBSTITUTE NOTIFICA-
24 TION.—Such substitute notification shall in-
25 clude—

(i) email notification to the extent that the person has email addresses of individuals to whom it is required to provide notification under subsection (a)(1);

(ii) a conspicuous notice on the Internet website of the person (if such person maintains such a website); and

(iii) notification in print and to broadcast media, including major media in metropolitan and rural areas where the individuals whose personal information was acquired reside.

(C) CONTENT OF SUBSTITUTE NOTICE.—

Each form of substitute notice under this paragraph shall include—

- (i) notice that individuals whose personal information is included in the breach of security are entitled to receive, at no cost to the individuals, consumer credit reports on a quarterly basis for a period of 5 years, credit monitoring or other service that enables consumers to detect the misuse of their personal information for a period of 10 years, and instructions on requesting such reports or service from the

1 person, except when the only information
2 which has been the subject of the security
3 breach is the individual's first name or ini-
4 tial and last name, or address, or phone
5 number, in combination with a credit or
6 debit card number, and any required secu-
7 rity code; and

8 (ii) a telephone number by which an
9 individual can, at no cost to such indi-
10 vidual, learn whether that individual's per-
11 sonal information is included in the breach
12 of security.

13 (3) REGULATIONS AND GUIDANCE.—

14 (A) REGULATIONS.—Not later than 1 year
15 after the date of enactment of this Act, the
16 Commission shall, by regulation under section
17 553 of title 5, United States Code, establish cri-
18 teria for determining circumstances under
19 which substitute notification may be provided
20 under paragraph (2), including criteria for de-
21 termining if notification under paragraph (1) is
22 not feasible due to excessive costs to the person
23 required to provide such notification relative to
24 the resources of such person. Such regula-
25 tions may also identify other circumstances

where substitute notification would be appropriate for any person, including circumstances under which the cost of providing notification exceeds the benefits to consumers.

17 (e) OTHER OBLIGATIONS FOLLOWING BREACH.—

18 (1) IN GENERAL.—A person required to provide
19 notification under subsection (a) shall, upon request
20 of an individual whose personal information was in-
21 cluded in the breach of security, provide or arrange
22 for the provision of, to each such individual and at
23 no cost to such individual—

24 (A) consumer credit reports from at least
25 one of the major consumer reporting agencies

beginning not later than 30 days following the individual's request and continuing on a quarterly basis for a period of 10 years thereafter; or

(B) a credit monitoring or other service that enables consumers to detect the misuse of their personal information, beginning not later than 30 days following the individual's request and continuing for a period of 10 years.

(2) LIMITATION.—This subsection shall not apply if the only personal information which has been the subject of the security breach is the individual's first name or initial and last name, or address, or phone number, in combination with a credit or debit card number, and any required security code.

(3) RULEMAKING.—As part of the Commission's rulemaking described in subsection (d)(3), the Commission shall determine the circumstances under which a person required to provide notification under subsection (a)(1) shall provide or arrange for the provision of free consumer credit reports or credit monitoring or other service to affected individuals.

(4) BREACH OF CONSUMER REPORTING AGENCY.—In the event of a breach of security of a consumer reporting agency, that agency shall provide

1 any consumer credit report required under para-
2 graph (1)(A) from another consumer reporting agen-
3 cy.

4 (f) EXEMPTION.—

5 (1) GENERAL EXEMPTION.—A person shall be
6 exempt from the requirements under this section if,
7 following a breach of security, such person deter-
8 mines that there is no reasonable risk of identity
9 theft, fraud, or other unlawful conduct.

10 (2) PRESUMPTION.—

11 (A) IN GENERAL.—If the data in electronic
12 form containing personal information is ren-
13 dered unusable, unreadable, or indecipherable
14 through encryption or other security technology
15 or methodology (if the method of encryption or
16 such other technology or methodology is gen-
17 erally accepted by experts in the information se-
18 curity field), there shall be a presumption that
19 no reasonable risk of identity theft, fraud, or
20 other unlawful conduct exists following a breach
21 of security of such data. Any such presumption
22 may be rebutted by facts demonstrating that
23 the encryption or other security technologies or
24 methodologies in a specific case, have been or
25 are reasonably likely to be compromised.

(B) METHODOLOGIES OR TECH-
NOLOGIES.—Not later than 1 year after the date of the enactment of this Act and biannually thereafter, the Commission shall issue rules (pursuant to section 553 of title 5, United States Code) or guidance to identify security methodologies or technologies which render data in electronic form unusable, unreadable, or indecipherable, that shall, if applied to such data, establish a presumption that no reasonable risk of identity theft, fraud, or other unlawful conduct exists following a breach of security of such data. Any such presumption may be rebutted by facts demonstrating that any such methodology or technology in a specific case has been or is reasonably likely to be compromised. In issuing such rules or guidance, the Commission shall consult with relevant industries, consumer organizations, and data security and identity theft prevention experts and established standards setting bodies.

(3) FTC GUIDANCE.—Not later than 1 year after the date of the enactment of this Act the Commission shall issue guidance regarding the application of the exemption in paragraph (1).

1 (g) WEBSITE NOTICE OF FEDERAL TRADE COMMIS-
2 SION.—If the Commission, upon receiving notification of
3 any breach of security that is reported to the Commission
4 under subsection (a)(2), finds that notification of such a
5 breach of security via the Commission’s Internet website
6 would be in the public interest or for the protection of
7 consumers, the Commission shall place such a notice in
8 a clear and conspicuous location on its Internet website.

9 (h) WEBSITE NOTICE OF CONSUMER FINANCIAL
10 PROTECTION BUREAU.—If the Bureau, upon receiving no-
11 tification of any breach of security that is reported to the
12 Bureau under subsection (a)(2), finds that notification of
13 such a breach of security via the Bureau’s Internet website
14 would be in the public interest or for the protection of
15 consumers, the Bureau shall place such a notice in a clear
16 and conspicuous location on its Internet website.

17 (i) FTC STUDY ON NOTIFICATION IN LANGUAGES IN
18 ADDITION TO ENGLISH.—Not later than 1 year after the
19 date of enactment of this Act, the Commission, in con-
20 sultation with the Bureau, shall conduct a study on the
21 practicality and cost effectiveness of requiring the notifica-
22 tion required by subsection (d)(1) to be provided in a lan-
23 guage in addition to English to individuals known to speak
24 only such other language.

1 (j) GENERAL RULEMAKING AUTHORITY.—The Com-
2 mission and Bureau may promulgate regulations nec-
3 essary under section 553 of title 5, United States Code,
4 to effectively enforce the requirements of this section.

5 (k) TREATMENT OF PERSONS GOVERNED BY OTHER
6 LAW.—A person who is in compliance with any other Fed-
7 eral law that requires such person to provide notification
8 to individuals following a breach of security, and that,
9 taken as a whole, provides protections substantially similar
10 to, or greater than, those required under this section, as
11 the Commission shall determine by rule (under section
12 553 of title 5, United States Code), shall be deemed to
13 be in compliance with this section.

14 **SEC. 2. APPLICATION AND ENFORCEMENT.**

15 (a) ENFORCEMENT BY THE FEDERAL TRADE COM-
16 MISSION.—

17 (1) UNFAIR OR DECEPTIVE ACTS OR PRAC-
18 TICES.—A violation of section 1 shall be treated as
19 an unfair and deceptive act or practice in violation
20 of a regulation under section 18(a)(1)(B) of the
21 Federal Trade Commission Act (15 U.S.C.
22 57a(a)(1)(B)) regarding unfair or deceptive acts or
23 practices.

24 (2) POWERS OF COMMISSION.—The Commis-
25 sion shall enforce this Act in the same manner, by

1 the same means, and with the same jurisdiction,
2 powers, and duties as though all applicable terms
3 and provisions of the Federal Trade Commission Act
4 (15 U.S.C. 41 et seq.) were incorporated into and
5 made a part of this Act. Any person who violates
6 such regulations shall be subject to the penalties and
7 entitled to the privileges and immunities provided in
8 that Act.

9 (3) LIMITATION.—In promulgating rules under
10 this Act, the Commission shall not require the de-
11 ployment or use of any specific products or tech-
12 nologies, including any specific computer software or
13 hardware.

14 (b) ENFORCEMENT BY STATE ATTORNEYS GEN-
15 ERAL.—

16 (1) CIVIL ACTION.—In any case in which the
17 attorney general of a State, or an official or agency
18 of a State, has reason to believe that an interest of
19 the residents of that State has been or is threatened
20 or adversely affected by any person who violates sec-
21 tion 1 of this Act, the attorney general, official, or
22 agency of the State, as parens patriae, may bring a
23 civil action on behalf of the residents of the State in
24 a district court of the United States of appropriate
25 jurisdiction—

- 1 (A) to enjoin further violation of such sec-
2 tion by the defendant;
3 (B) to compel compliance with such sec-
4 tion; or
5 (C) to obtain civil penalties in the amount
6 determined under paragraph (2).

7 (2) CIVIL PENALTIES.—

8 (A) CALCULATION.—For purposes of para-
9 graph (1)(C) with regard to a violation of sec-
10 tion 1, the amount determined under this para-
11 graph is the amount calculated by multiplying
12 the number of violations of such section by an
13 amount not greater than \$11,000. Each failure
14 to send notification as required under section 3
15 to a resident of the State shall be treated as a
16 separate violation.

17 (B) ADJUSTMENT FOR INFLATION.—Be-
18 ginning on the date that the Consumer Price
19 Index is first published by the Bureau of Labor
20 Statistics that is after 1 year after the date of
21 enactment of this Act, and each year thereafter,
22 the amounts specified in clause (i) of subpara-
23 graph (A) shall be increased by the percentage
24 increase in the Consumer Price Index published

1 on that date from the Consumer Price Index
2 published the previous year.

3 (C) MAXIMUM TOTAL LIABILITY.—Not
4 withstanding the number of actions which may
5 be brought against a person under this sub-
6 section, the maximum civil penalty for which
7 any person may be liable under this subsection
8 shall not exceed—

- 9 (i) \$5,000,000 for each violation of
10 section 2; and
11 (ii) \$5,000,000 for all violations of
12 section 3 resulting from a single breach of
13 security.

14 (3) INTERVENTION BY THE FTC.—

15 (A) NOTICE AND INTERVENTION.—The
16 State shall provide prior written notice of any
17 action under paragraph (1) to the Commission
18 and provide the Commission with a copy of its
19 complaint, except in any case in which such
20 prior notice is not feasible, in which case the
21 State shall serve such notice immediately upon
22 instituting such action. The Commission shall
23 have the right—

- 24 (i) to intervene in the action;

13 (4) CONSTRUCTION.—For purposes of bringing
14 any civil action under paragraph (1), nothing in this
15 Act shall be construed to prevent an attorney gen-
16 eral of a State from exercising the powers conferred
17 on the attorney general by the laws of that State
18 to—

24 (c) AFFIRMATIVE DEFENSE FOR A VIOLATION OF
25 SECTION 1—

1 (1) IN GENERAL.—It shall be an affirmative de-
2 fense to an enforcement action brought under sub-
3 section (a), or a civil action brought under sub-
4 section (b), based on a violation of section 1, that
5 all of the personal information contained in the data
6 in electronic form that was acquired or accessed as
7 a result of a breach of security of the defendant is
8 public record information that is lawfully made
9 available to the general public from Federal, State,
10 or local government records and was acquired by the
11 defendant from such records.

12 (2) NO EFFECT ON OTHER REQUIREMENTS.—
13 Nothing in this subsection shall be construed to ex-
14empt any person from the requirement to notify the
15 Commission of a breach of security as required
16 under section 3(a).

17 **SEC. 3. PROHIBITION ON CERTAIN CONTRACT CLAUSES.**

18 (a) UNLAWFUL CONDUCT.—It shall be unlawful for
19 any person to include a clause in a contract that—

20 (1) prohibits an individual described in section
21 (1)(a)(1) from pursuing civil action related to the
22 breach; or

23 (2) requires mandatory arbitration related to
24 the breach.

1 (b) VIOLATION OF RULE.—A violation of subsection
2 (a) shall be treated as a violation of a rule defining an
3 unfair or deceptive act or practice prescribed under section
4 18(a)(1)(B) of the Federal Trade Commission Act (15
5 U.S.C. 57a(a)(1)(B)).

6 (c) POWERS OF COMMISSION.—The Commission shall
7 enforce this section in the same manner, by the same
8 means, and with the same jurisdiction, powers, and duties
9 as though all applicable terms and provisions of the Fed-
10 eral Trade Commission Act (15 U.S.C. 41 et seq.) were
11 incorporated into and made a part of this Act. Any person
12 who violates subsection (a) shall be subject to the penalties
13 and entitled to the privileges and immunities provided in
14 the Federal Trade Commission Act.

15 **SEC. 4. DEFINITIONS.**

16 In this Act:

17 (1) BREACH OF SECURITY.—The term “breach
18 of security” means the unauthorized acquisition of
19 data in electronic form containing personal informa-
20 tion.

21 (2) BUREAU.—The term “Bureau” means the
22 Consumer Financial Protection Bureau.

23 (3) COMMISSION.—The term “Commission”
24 means the Federal Trade Commission.

1 (4) CONSUMER REPORTING AGENCY.—The term
2 “consumer reporting agency” has the meaning given
3 the term “consumer reporting agency that compiles
4 and maintains files on consumers on a nationwide
5 basis” in section 603(p) of the Fair Credit Report-
6 ing Act (15 U.S.C. 1681a(p)).

7 (5) DATA IN ELECTRONIC FORM.—The term
8 “data in electronic form” means any data stored
9 electronically or digitally on any computer system or
10 other database and includes recordable tapes and
11 other mass storage devices.

12 (6) ENCRYPTION.—The term “encryption”
13 means the protection of data in electronic form in
14 storage or in transit using an encryption technology
15 that has been adopted by an established standards
16 setting body which renders such data indecipherable
17 in the absence of associated cryptographic keys nec-
18 essary to enable decryption of such data. Such
19 encryption must include appropriate management
20 and safeguards of such keys to protect the integrity
21 of the encryption.

22 (7) IDENTITY THEFT.—The term “identity
23 theft” means the unauthorized use of another per-
24 son’s personal information for the purpose of engag-

1 ing in commercial transactions under the name of
2 such other person.

3 (8) NON-PUBLIC INFORMATION.—The term
4 “non-public information” means information about
5 an individual that is of a private nature and neither
6 available to the general public nor obtained from a
7 public record.

8 (9) PERSONAL INFORMATION.—

9 (A) DEFINITION.—The term “personal in-
10 formation” means any information or compila-
11 tion of information that includes any of the fol-
12 lowing:

13 (i) An individual’s first name or initial
14 and last name in combination with any or
15 more of the following data elements for
16 that individuals:

17 (I) Home address or telephone
18 number.

19 (II) Mother’s maiden name.

20 (III) Month, day, and year of
21 birth.

22 (IV) User name or electronic
23 mail address.

24 (ii) Driver’s license number, passport
25 number, military identification number,

1 alien registration number, or other similar
2 number issued on a government document
3 used to verify identity.

4 (iii) Unique account identifier, includ-
5 ing a financial account number, credit or
6 debit card number, electronic identification
7 number, user name, or routing code.

8 (iv) Partial or complete Social Secu-
9 rity number.

10 (v) Unique biometric or genetic data
11 such as a fingerprint, voice print, a retina
12 or iris image, or any other unique physical
13 representations.

14 (vi) Information that could be used to
15 access an individual's account, such as
16 user name and password or email address
17 and password.

18 (vii) Any two or more of the following
19 data elements:

20 (I) An individual's first and last
21 name or first initial and last name.

22 (II) A unique account identifier,
23 including a financial account number
24 or credit or debit card number, elec-

1 electronic identification number, user
2 name, or routing code.

3 (III) Any security code, access
4 code, or password, or source code that
5 could be used to generate such codes
6 or passwords.

7 (viii) Information generated or derived
8 from the operation or use of an electronic
9 communications device that is sufficient to
10 identify the street name and name of the
11 city or town in which the device is located.

12 (ix) Any information regarding an in-
13 dividual's medical history, mental or phys-
14 ical condition, medical treatment or diag-
15 nosis by a health care professional, or the
16 provision of health care to the individual,
17 including health information provided to a
18 website or mobile application.

1 (xi) Digitized or other electronic sig-
2 nature.

(xii) Nonpublic communications or other user-created content such as emails, photographs, or videos.

12 (xiv) Any additional element the Com-
13 mission defines as personal information.

(10) PUBLIC RECORD INFORMATION.—The term “public record information” means information about an individual which has been obtained originally from records of a Federal, State, or local government entity that are available for public inspection.

1 (11) SERVICE PROVIDER.—The term “service
2 provider” means an entity that provides to a user
3 transmission, routing, intermediate and transient
4 storage, or connections to its system or network, for
5 electronic communications, between or among points
6 specified by such user of material of the user’s
7 choosing, without modification to the content of the
8 material as sent or received. Any such entity shall
9 be treated as a service provider under this Act only
10 to the extent that it is engaged in the provision of
11 such transmission, routing, intermediate and tran-
12 sient storage, or connections.

13 (12) STATE.—The term “State” means each of
14 the several States, the District of Columbia, the
15 Commonwealth of Puerto Rico, Guam, American
16 Samoa, the United States Virgin Islands, the Com-
17 monwealth of the Northern Mariana Islands, any
18 other territory or possession of the United States,
19 and each federally recognized Indian Tribe.

20 **SEC. 5. EFFECT ON OTHER LAWS.**

21 (a) PREEMPTION OF STATE INFORMATION SECURITY
22 LAWS.—This Act supersedes any provision of a statute,
23 regulation, or rule of a State or political subdivision of
24 a State, with respect to those entities covered by the regu-
25 lations issued pursuant to this Act, that expressly requires

1 notification to individuals of a breach of security resulting
2 in unauthorized access to or acquisition of data in elec-
3 tronic form containing personal information.

4 (b) ADDITIONAL PREEMPTION.—

5 (1) IN GENERAL.—No person other than a per-
6 son specified in section 2(b) may bring a civil action
7 under the laws of any State if such action is pre-
8 mised in whole or in part upon the defendant vio-
9 lating any provision of this Act.

10 (2) PROTECTION OF CONSUMER PROTECTION
11 LAWS.—This subsection shall not be construed to
12 limit the enforcement of any State consumer protec-
13 tion law by an attorney general of a State.

14 (c) PROTECTION OF CERTAIN STATE LAWS.—This
15 Act shall not be construed to preempt the applicability
16 of—

17 (1) State trespass, contract, or tort law; or
18 (2) other State laws to the extent that those
19 laws relate to acts of fraud.

20 (d) PRESERVATION OF FTC AUTHORITY.—Nothing
21 in this Act may be construed to limit or affect the Com-
22 mission's authority under any other provision of law.

23 **SEC. 6. EFFECTIVE DATE.**

24 This Act shall take effect 1 year after the date of
25 enactment of this Act.

1 SEC. 7. AUTHORIZATION OF APPROPRIATIONS.

2 There is authorized to be appropriated to the Com-
3 mission \$1,000,000 for each of fiscal years 2018 through
4 2023 to carry out this Act.

